OPENING STATEMENT OF CHAIRMAN SPENCER BACHUS
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT
"ENHANCING DATA SECURITY: THE REGULATORS' PERSPECTIVE"
MAY 18, 2005

Good morning. The Subcommittee will come to order. This morning the subcommittee will continue its examination of data security and protecting sensitive information. Several weeks ago, the Full Committee held a hearing on this topic where we heard from representatives of companies that recently experienced data breaches. Today it is our intention to hear the regulators' perspective on this issue. I am pleased that Chairman Oxley continues to recognize the significance of this topic and has scheduled this hearing today.

Over the last several months, there have been numerous news reports describing potentially serious breaches of information security. These breaches have generally involved sensitive personal information, such as individual names plus Social Security numbers or payment card information. Although the reports of subsequent fraud associated with these breaches have been relatively low, protecting consumers after such data breaches obviously remains a primary concern. Furthermore, data breaches, even if relatively uncommon and limited in scope, undermine consumer confidence more broadly. For instance, surveys suggest the growth of on-line commerce is restrained due to fears about information security.

I do not expect companies to meet a standard of perfection. I doubt the witnesses here expect perfection either. Even the most prudent company can become the victim of a hacker or other criminal. However, it is reasonable to

expect that those who possess sensitive information will take reasonable steps to protect against the unauthorized acquisition of such information. In this regard, it is important for us to hear how the regulatory community is approaching this issue, and whether additional legislation is needed. It is also reasonable to expect that, if we decide to legislate in this area, companies should have a single uniform standard to comply with, as opposed to dozens of inconsistent standards. I see little benefit to a hodgepodge of security standards resulting from several different laws triggering consumer notices.

One of the key issues surrounding our investigation of data breaches is a question of how to inform consumers if their sensitive information is the subject of a security breach. For example, we are well aware that financial institutions must have information security programs designed to protect customer information under the Gramm-Leach-Bliley Act. The federal banking agencies also issued guidance recently with respect to the need for a bank to provide notice to its customers when information in the bank's control is the subject of a security breach. In my opinion the requirements of the law, and the guidance provided by the regulators, are appropriate. However, we need to learn more about this issue from the regulators, and that is why we are here today.

I would like to take this opportunity to welcome our witnesses. We have with us today FTC Director of the Bureau of Consumer Protection Lydia B. Parnes, FDIC Deputy Director of the Division of Supervision and Consumer Protection Sandra Thompson and NCUA General Counsel Robert Fenner. I look forward to hearing from today's witnesses and thank them for taking time from their schedules to join us.

I am now pleased to recognize the Ranking Member, Mr. Sanders, for any opening statement that he would like to make.